Remarks/Arguments:

I. Status

The Office Action dated December 28, 2004 (the "Office Action") has been carefully reviewed. Claims 1, 8, 9 and 13 have been amended. Claims 21-25 have been added. Accordingly, claims 1-25 are pending in this application. Reconsideration of this application, as amended, is respectfully requested.

II. The Rejection of Claims 1-20 under 35 U.S.C. § 101 Should be Withdrawn.

Discussion re: Claims 1, 8 and 15

In the Office Action, claims 1-20 were rejected under 35 U.S.C. § 101 as being directed to non-statutory subject matter and for lacking patentable utility. The Applicant respectfully traverses.

Specifically, the Examiner has alleged that claims 1, 8 and 15 "are dedicated to the abstract idea of an algorithm for generating messages without a practical utility (i.e. lacks utility)." (Office Action at page 2, citing to the MPEP § 2106 at pages 10 and 11). The MPEP recognizes the requirement that any new and useful process, machine, manufacture or composition is the proper subject matter of a patent. (MPEP § 2106 at page 11.) Moreover, the MPEP states that in determining whether or not the invention is useful, the Examiner "*will* review the complete specification, including the detailed description of the invention, any specific embodiments that have been disclosed, the claims and any specific, substantial, and credible utilities that have been asserted for the invention." (MPEP § 2106 at page 6 (emphasis added)).

Claims 1, 8 and 15 are all directed to the generation and transmission of bogus messages between a terminal and a host computer in a wireless network. As clearly set forth in the specification, the generation of bogus messages in a wireless retail store environment is very useful. Specifically, at page 6, lines 12-21 the Specification states:

> The bogus message traffic camouflages the bona fide transactional message traffic flow so the usefulness of the data that may be gleaned from analyzing transactional data flow is degraded. Additionally, those persons eavesdropping on the store wireless communication traffic to obtain data for generating identification and financial transaction tokens are probably unable to distinguish valid transaction messages from bogus messages. Consequently, the interception of data messages from a wireless system incorporating the system and method of the present invention is rendered less profitable and useful for the manufacture of counterfeit tokens.

Therefore, the Specification clearly sets forth specific, substantial, and credible utilities for the inventions of claim 1, 8 and 15. In contrast, even though the MPEP § 2106 at page 7 places the burden of establishing non-utility on the Examiner, the Office Action fails to identify any evidence that the generation of bogus messages in a wireless retail store environment is not useful.

Accordingly, because the Specification identifies the utility of the invention of claims 1, 8 and 15, and because the Examiner has failed to identify any evidence that the claimed invention is not useful, a *prima facie* case of non-utility has not been made and the rejection of claims 1, 8 and 15 under 35 U.S.C. § 101 should be withdrawn.

Discussion re: Claims 2-7, 9-14 and 16-20

Claims 2-7, 9-14 and 16-20 depend from claims 1, 8 or 15 and include all of the limitations of the claims from which they depend. Therefore, the inventions identified in claims 2-7, 9-14 and 16-20 are useful for at least the same reasons discussed above with

respect to claims 1, 8 and 15 and the rejection of claims 2-7, 9-14 and 16-20 under 35 U.S.C. § 101 should be withdrawn.

III. The Rejection of Claims 1-7 under 35 U.S.C. § 112 Has Been Overcome.

In the Office Action, claims 1 was rejected under 35 U.S.C. § 112 as being incomplete for omitting an essential step and claims 2-6 were rejected as depending from claim 1. The Applicant has amended claim 1 to clarify the interrelationship between components recited in the claim.

Specifically, the Examiner has alleged that claim 1 omits the "step" of the host computer transmitting a message to the bogus message generator to create a bogus message which is alleged to be essential because the bogus message generator requires a trigger. (Office Action at page 3). Claim 1 has been amended to clarify that the communication parameter regulator is operable to activate the bogus message generator.

Claim 1, as amended, recites the interrelationship between the communication parameter regulator and the bogus message generator. Accordingly, it is respectfully submitted that the Examiner's rejection of claims 1-7 under 35 U.S.C. § 112 has been overcome.

IV. The Rejection of Claims 1-20 under 103(a) Should be Withdrawn.

In the Office Action, claims 1-20 were rejected under 35 U.S.C. 103(a) as being obvious over International Publication No. WO/200046959 of Nordenstam et al. (hereinafter "Nordenstam") in view of U.S. Patent No. 4,262,359 of Cory et al. (hereinafter "Cory") and U.S. Patent No. 6,502,135 B1 to Munger et al. (hereinafter Munger"). The Applicant respectfully traverses.

The Present Invention

The present invention relates generally to methods and systems for implementing financial transactions in a retail store and, more particularly, to methods and systems for implementing financial transactions in a retail store through a store host network.

In accordance with one embodiment, a communication parameter regulator determines the number of transaction messages being received at a store host computer. The communication parameter regulator then determines the load on the store host computer using the average length of time required for the store host computer to process the received transaction messages and the average time between receipt of transaction messages by the store host computer.

In the event that the load on the store host computer is below a predetermined level, the communication parameter regulator generates a bogus message request. The bogus message request is transmitted to a transaction terminal that is operable to wirelessly transmit transaction messages to the store host computer. A bogus message generator associated with the transaction terminal generates a bogus message in response to the bogus message request and the transaction terminal transmits the bogus message to the store host computer.

In accordance with further embodiments, the generation of bogus messages may continue for a predetermined amount of time. Alternatively or additionally, the transmission of bogus messages from the transaction terminal may be stopped when it is determined that the transaction terminal is engaged in an actual transaction.

Nordenstam

Nordenstam discloses a system wherein mobile terminals are used in a wireless transaction network. (Nordenstam at Abstract). Nordenstam discloses two network environments in which the disclosed system may be used. FIG. 3 depicts transaction terminals 22, 24 and 26 within a single local area network (LAN). (Id. at page 15, lines 10-17). FIG. 4 of Nordenstam depicts transaction terminals 22, 24 and 26 that are located

in and operated by different stores. (See Id. at page 19, lines 4-15). Thus, FIG. 4 shows the operation of three separate but partially overlapping LANs. Nordenstam teaches a system that can be used in either environment to provide service card transactions over the wireless network.

Specifically, mobile terminals and transaction terminals are configured with BLUETOOTH® capability. (Id. at page 15, lines 4-6). BLUETOOTH® capability allows for multiple devices to communicate in a wireless environment by creating so-called piconets. In a piconet, one of the devices operates as a master device and the remaining devices act as slave devices. Accordingly, in the single LAN environment of FIG. 3, transaction terminal 22 operates as the master of the piconet or LAN. (Id. at page 15, lines 11-17). The master transaction terminal 22 is shown hardwired to the host computer 32. (Id. at page 15, lines 11-17). In the three LAN system of FIG. 4, each of the transaction terminals 22, 24 and 26 may be configured as a master terminal or another terminal (not shown) may be the master terminal. (Id. at page 18, lines 6-15). Each LAN in FIG. 4 operates as an independent piconet.

In either environment, a mobile telephone or personal digital assistant (PDA) may be used as a "mobile terminal" to access the store's network. (Id. at page 9, lines 12-15). Specifically, when the mobile terminal 10 enters into the range of a master terminal, a piconet is formed that includes the master terminal and the mobile terminal 10 in accordance with standard BLUETOOTH® protocol. (Id. at page 14, lines 12-22).

BLUETOOTH® devices comply with a standardized communications protocol, the description of which is available through the Internet site at **www.bluetooth.com**. A short excerpt of the *Specification of the Bluetooth System* available through that site is attached hereto for the Examiner's convenience. As set forth in that excerpt, when a

piconet is established, communication is controlled by the master device. Specifically, the master establishes both the clock and the hopping pattern for all of the devices in the piconet. (*Specification of the Bluetooth System*, version 1.2, volume 1, at page 32). The master device also controls access to the physical data communications channel. (Id. at page 32). Accordingly, a slave device in a piconet is only allowed to transmit data to the master device of the piconet during certain restricted timeframes.

Therefore, Nordenstam teaches a system wherein a master terminal establishes communications with slave terminals. The communications may be relatively permanent for less mobile slave terminals (transaction terminals) or the communications may be established as the slave terminals (mobile telephones and/or PDAs) enter the range of the master terminal. In either event, the slave terminals are only allowed to transmit data to the master terminal at specified times established by the master terminal, i.e. the slaves cannot transmit data to the master continuously.

Cory

Cory discloses a cryptographic unit for automatically inserting dummy data into a transmitter when there is no valid character to be transmitted. (Cory at column 1, lines 19-23). The system of Cory first determines whether or not any valid data is available for transmission. (Id. at column 4, lines 2-5). If data is available, the data is transmitted. (Id. at column 4, lines 2-6). In the event there is no data, a "V" generator 58 is activated and a series of five characters or dummy data is transmitted in the form of five "V"s. (Id. at column 4, lines 15-19). At the completion of transmitting the fifth dummy data character, the system once again determines whether or not any valid data is available for

transmission and repeats the sending of five characters (dummy data) if there is no valid data. (Id. at column 4, lines 21-24).

Accordingly Cory discloses a transmitter that automatically transmits a set of five characters (dummy data) whenever there is no valid data to transmit. The result is that anyone looking at the transmission line from the transmitter would not see any change in the traffic volume over the transmission line. (Id. at column 4, lines 28-30). In other words, the transmitter of Cory is continuously transmitting, regardless of the availability of valid data or any conditions on the transmission line. Moreover, the determination of whether or not to transmit the dummy data is based solely on whether or not valid data is available for transmission. The activity, if any, on the receiving portion of the terminal is not considered.

Munger

Munger is directed to a mechanism that includes a special routing protocol and special terminals/routers to provide security and anonymity for communications over the Internet. (Munger at column 1, lines 16-18 and column 2, line 66 through column 3, lines 3). The protocol is referred to as Tunneled Agile Routing Protocol (TARP) and the special terminals/routers are TARP terminals/routers. (Munger at column 2, line 66 through column 3, lines 3). Munger discloses various schemes to inhibit "traffic analysis". "Traffic analysis" is a method of establishing the identity of two communicating terminals within a network by tracking the amount of traffic at each of the terminals in the network. (See e.g. Id. at column 1, line 65 through column 2, line 24).

One scheme disclosed by Munger for inhibiting traffic analysis is the manner in which IP packets are exchanged between TARP terminals/routers. Specifically, the TARP terminals exchange IP packets whose ultimate destination address is hidden except to other TARP terminals and TARP routers. (Id. at column 3, lines 3-8). This is accomplished by encrypting the ultimate destination within the IP packet and then "hopping" the encrypted packet to random TARP routers using the unencrypted IP address of the randomly selected router. (Id. at column 3, lines 29-36). Each TARP router that receives a package decrypts the encrypted destination address. If the receiving TARP router is not the ultimate router address for the packet, the packet is hopped to another random TARP router. This continues until the last hop, wherein the ultimate destination is also set as the unencrypted address. Thus, the destination address of the IP packet is simply the next TARP router in a series of hops between TARP routers or the destination TARP router. (Id. at column 3, lines 11-13). Accordingly, even if an IP packet is intercepted, the only information available is the next TARP router, which may or may not be the destination TARP router. (Id. at column 3, lines 13-17).

Traffic analysis is further inhibited in the system of Munger by the insertion/deletion of dummy data. For example, dummy data may be inserted into the IP packets along with the actual data. (Id. at column 4, lines 35-37). This allows for a larger number of IP packets to be constructed, each of which will be routed differently. (Id. at column 4, lines 43-46). Additionally, IP packets which are totally comprised of dummy data (dummy packets) may be constructed to reduce the peak-to-average network load. (Id. at column 4, lines 35-38). This also allows for communications bursts between communicating devices to be hidden by increasing the overall traffic on the network. (Id. at column 4, lines 38-43). To further camouflage the actual endpoints of the

communications, the TARP terminals/routers may drop dummy packets as well as generate dummy packets so as to obscure the actual number of incoming and outgoing packets from the particular TARP terminal/router. (Id. at column 5, lines 44-48).

The control mechanism disclosed for effecting the generation and dropping of packets at a TARP terminal/router is an algorithm. (Id. at column 12, lines 26-28). The algorithm may be based upon random generation, time of day or by detection of the terminal being idle. (Id. at column 12, lines 28-33). Munger also states that the algorithm may be responsive to "low traffic times". (Id. at column 12, lines 31-33). Munger does not define what is meant by "low traffic times". Thus, this term, without further context, could be taken to mean low traffic times at the tarp terminal/router or low traffic times on the network. However, in the context of the disclosure of Munger, it is clear that the "low traffic" is the traffic at the particular TARP terminal/router. Thus, each terminal monitors its own traffic and drops or adds dummy packets and/or dummy data based upon its own internal algorithm.

Specifically, all of the discussion in the passage from column 12, line 26 to column 14, line 38, is directed to the actions of an individual TARP terminal (or router). Moreover, FIG. 5 depicts the particular steps of the method of Munger. (Id. at column 12, lines 58-61). Significantly, the steps include a background loop operation that applies the algorithm that controls generation or dropping of dummy packets and insertion of dummy data. (Id. at FIG. 5 and column 12, lines 62-65). As discussed in Munger, the background loop is "interrupted when an encrypted TARP package is received." (Id. at column 12, lines 62-65). The remaining steps then depict the actions taken *by the TARP terminal/router* to process the received packet. (Id. at column 12, line 66 through column 13, line 38). Clearly, the algorithm is running on the TARP terminal/router. Moreover,

there is no teaching or suggestion that any TARP terminal/router is monitoring another TARP terminal/router or that any TARP terminal/router is interacting with or monitored and controlled by some other component. Therefore, the "low traffic times" obviously refer to low traffic at the particular TARP terminal/router.

Accordingly, Munger discloses a system wherein each TARP terminal/router monitors the number of packets it is receiving and sending and modifies the number of packets it is transmitting by generating dummy packets or dropping received dummy packets.

A. There is No Motivation for the Proposed Combinations

1. There is No Motivation to Modify Nordenstam With Cory.

In the rejection of claims 1-20, the Examiner has relied upon Nordenstam for teaching a system for transmitting from a wireless terminal to a host computer. (Office Action at page 4). The Examiner has further proposed modifying the system of Nordenstam to incorporate the "bogus message generator" and transmission of "bogus messages" as taught by Cory. (Office Action at page 4). Respectfully, such a modification of Nordenstam changes the principle of operation of Nordenstam.

Specifically, as discussed above, Nordenstam teaches a system that uses BLUETOOTH® technology. Accordingly, the system requires slave terminals to *not* transmit continuously to the master. In contrast, the terminal in the system of Cory, as discussed above, is configured to *continuously* transmit data, either real or bogus. The Examiner has not explained how the architecture of Nordenstam could be changed to incorporate a plurality of continuously transmitting slave devices in a piconet.

Nonetheless, it is clear that any such redesign would necessarily change the principle of operation of the system disclosed by Nordenstam.

If the proposed modification or combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims *prima facie* obvious. *In re Ratti*, 270 F.2d 810, (CCPA 1959). Therefore, because the proposed modification would change the principle of operation of the system of Nordenstam from a BLUETOOTH® technology based system to some other undefined and incompatible system, there is no suggestion or motivation for the proposed modification of Nordenstam with Cory as proposed by the Examiner. Because there is no suggestion or motivation for the proposed combination, a *prima facie* case of obviousness has not been made and the rejection of claims 1-20 under 35 U.S.C. § 103(a) should be withdrawn.

2. There is No Motivation for the Modification of Cory.

In the rejection of claims 1-20, the Examiner has stated that even modifying Nordenstam with the bogus message generation of Cory do not disclose monitoring a parameter *at the receiving end* of a transmission and using the monitored parameter as a trigger for the generation of a bogus message. (Office Action at page 5 (emphasis added)). The Examiner then sites to Munger as allegedly disclosing the element admittedly missing in the Nordenstam and Cory references. Respectfully, assuming *arguendo* that the Examiner's characterization of Munger is correct, the proposed modification renders Cory unsatisfactory for its intended purpose.

Specifically, the Examiner has characterized Munger as teaching that bogus messages are generated based upon the monitoring of "network traffic conditions".

(Office Action at page 5). It is not clear what the Examiner meant by "network traffic conditions" as is discussed more fully below. Nonetheless, in order to provide the monitoring of the end receiver that the Examiner has stated is missing from the other references, the Examiner apparently contends that Munger teaches monitoring network activity other than just the transmitting terminal activity. Therefore, in accordance with the proposed modification, it appears that a bogus message would only be generated when two conditions are met. First, the terminal would not be active and second, the level of communications on or at some point of the network other than at the transmitting terminal would be below the desired level of activity.

Obviously, there would be no need of a trigger based upon monitoring the level of communications on or at some point of the network other than at the transmitting terminal if the transmitting terminal was continuously transmitting either real or bogus data. Therefore, it follows that a terminal in the proposed system does not transmit if 1) there is no real data to transmit and 2) there is already sufficient traffic on the network at the monitoring point. Accordingly, transmitting terminals in the proposed system do not continuously transmit.

However, the stated object of Cory is to "provide continuous traffic". (Cory at column 1, lines 41-42). It is by ensuring that there are no inactive periods in transmission from a transmitter that Cory provides security. Specifically, "anyone looking at the transmission line would notice no change in traffic volume although the transmitter was off." (Cory at column 4, lines 28-30). Therefore, the proposed modification of Cory, to only send bogus messages when warranted by network conditions other than conditions at the transmitter, results in periods of inactivity at the transmitting terminal. Thus, the

proposed modification renders Cory unsatisfactory for its stated purpose of eliminating periods of inactivity at the transmitting terminal.

If a proposed modification would render the prior art invention being modified unsatisfactory for its intended purpose, then there is no suggestion or motivation to make the proposed modification. *In re Gordon*, 733 F.2d 900 (Fed. Cir. 1984). Accordingly, there is no suggestion or motivation for the proposed modification of Cory and Nordenstam with Munger as proposed by the Examiner. Because there is no suggestion or motivation for the proposed combination, a *prima facie* case of obviousness has not been made and the rejection of claims 1-20 under 35 U.S.C. § 103(a) should be withdrawn.

3. Conclusion

For any or all of the above reasons, it is respectfully submitted that there is no suggestion or motivation for the proposed modifications. Because there is no suggestion or motivation for the proposed combinations, a *prima facie* case of obviousness has not been made and the rejection of claims 1-20 under 35 U.S.C. § 103(a) should be withdrawn.

B. Claims 1-7 Are Patentable Over the Proposed Combination

Discussion re: Claim 1

1. Claim 1.

Claim 1, as amended, recites:

> A system for securing transactional data transmitted over a wireless network in a store comprising:
>
> a bogus message generator coupled to a wireless terminal in a store, the bogus message generator for generating bogus messages to be transmitted by the wireless terminal;

> a store host computer for receiving transactional and bogus messages from the wireless terminal; and
>
> a communication parameter regulator for measuring a communication parameter on the store host computer, the communication parameter regulator operable to activate the bogus message generator so that the bogus message generator is activated in accordance with the measured communication parameter.

Claim 1 thus recites a communication parameter regulator operable to measure a parameter at the receiving end of a transmission and to activate transmission of a bogus message to the receiving end based upon the measurement.

2. Prima Facie Obviousness Has Not Been Alleged.

The Examiner has admitted that the combination of Nordenstam and Cory does not teach or suggest all of the elements in claims 1-7. However, the Examiner has not identified any teaching or suggestion in Munger of the communication parameter regulator as recited in claim 1.

Specifically, in support of the proposition that Munger discloses a communication parameter regulator as claimed, the Examiner has merely stated that Munger discloses the monitoring of "network traffic conditions". (Id. at page 5). However, claim 1 recites that the communication parameter regulator is operable to measure a particular parameter at a specific location on the network, namely, *on the store host computer*. As discussed above, to the extent Munger discloses monitoring at any specific location, the monitoring is performed at the same TARP terminal/router that generates the bogus message. Obviously, monitoring network traffic conditions at the bogus message transmitter as is done in Munger is not the same as monitoring a particular parameter at a receiver of the transmitted bogus message as recited in claim 1.

Somewhat interestingly, the Office Action provides support of the Applicant's position. Specifically, the transmitter of Cory is a part of the network disclosed by Cory. Thus, Cory teaches monitoring network traffic since the traffic generated by the transmitter of Cory is monitored and used to trigger generation and transmission of bogus data by the transmitter. (See Cory at column 4, lines 1-17). However, as the Examiner has admitted, Cory does not teach or suggest monitoring a particular parameter at a receiver of the transmitted bogus message. Similarly, monitoring parameters at the TARP terminal/router of Munger an using that same TARP terminal/router to generate bogus data packets does not teach or suggest monitoring a particular parameter at a receiver of the transmitted bogus message.

Therefore, even accepting *arguendo* the proposed combination so as to include the monitoring of a network condition as disclosed in Munger, the Examiner has not alleged that the prior art teaches or suggests measuring a parameter at the receiving end of a transmission to activate transmission of a bogus message to the receiving end.[1] To properly allege a *prima facie* case of obviousness under MPEP § 2143, the prior art references must teach or suggest all the claim limitations. Accordingly, because the Examiner has failed to identify a communication parameter regulator as recited in claim 1 in the prior art, the Examiner has failed to present a *prima facie* case of obviousness and the rejection of claim 1 under 35 U.S.C. § 103(a) should be withdrawn.

---

[1] To the extent the Examiner intended the discussion on page 5 of the Office Action to be an allegation that Munger disclosed monitoring at some portion of the network other than a particular TARP terminal, such allegation is not well founded. Specifically, the Office Action at page 5 recites that "[t]he only requirements of the Munger et al. teaching is that the chosen algorithm generate bogus messages for foiling malicious traffic analysis efforts". However, even if this is true, it has no applicability to whether or not Munger *teaches or suggests* any limitations. More specifically, the statement neither teaches nor suggests the limitation of claim 1 of monitoring a parameter at a receiving component as required by MPEP § 2143.03.

Discussion Regarding Patentability of Claims 2-7

Claims 2-7 depend from claim 1 and include the same limitation discussed above with respect to claim 1 and additional limitations. Therefore, for at least the same reasons set forth above with respect to claim 1, claims 2-7 are allowable over the prior art.

Discussion Regarding Patentability of Claim 3

Claim 3 further recites a system with a bogus message generator that "terminates bogus message generation in response to a bogus message time expiration". The Examiner has not identified any such limitation in the prior art. Accordingly, in addition to the foregoing reasons, claim 3 is further allowable over the prior art.

Discussion Regarding Patentability of Claim 4

Claim 4 further recites a system with a bogus message generator that "terminates bogus message generation in response to a bona fide transaction occurring at the wireless terminal". The Examiner has not identified any such limitation in the prior art. Accordingly, in addition to the foregoing reasons, claim 4 is further allowable over the prior art.

C. Claims 8-14 Are Patentable Over the Proposed Combination

Discussion re: Claim 8

1. Claim 8.

Claim 8, as amended, recites:

> A method for securing transactional data communicated over a wireless network in a store comprising:
> determining dead space intervals on a store host computer based upon the store host computer load;
> generating bogus transactional messages for transmission over a wireless communication network for communicating data between the store host computer and a terminal located in a store; and
> transmitting the bogus transactional messages over the wireless communication network during the dead space intervals.

Claim 8 has been amended to clarify that the dead space intervals are dead space intervals at a host computer. Claim 8 thus recites determining when a store host computer is not operating at a certain capacity based upon an analysis of the receipt and processing of messages by the host computer.

2. Cory Does Not Disclose Determining Dead Space Intervals.

The Office Action states that Cory discloses the insertion of encrypted "bogus messages" during dead space between valid messages. (Office Action at page 4). Thus, Cory is apparently relied upon for teaching or suggesting the "dead space interval" recited in claim 8. Respectfully, the determination of "dead space" in Cory is not determining a dead space interval as recited in claim 8.

Specifically, neither the activity, if any, at the receiving portion of the Cory device nor the computational demands on the Cory device are considered in the determination. Thus, Cory determines whether or not dummy characters will be transmitted solely on determination of the availability of valid data for transmission.

As more clearly set forth in claim 8 as amended, determination of a "dead space interval" as recited in claim 8 incorporates a consideration of the amount of messages being received as well as the computational demands upon the store host computer. Specifically, the Specification at page 9 lines 9-11 clearly defines "load" as "the volume of message traffic expected from terminals 14a-14n during a communication interval and the estimated time required for processing the messages to generate response messages."

Cory neither teaches nor suggests consideration of either the transmitting terminal's load or the receiving terminal's load in determining whether or not to insert dummy data. Thus, the "dead space" insertion of Cory is not the same as the determination of "dead space intervals" as recited in claim 8.

Therefore, because the Cory does not teach or suggest the step of determining as claimed, a *prima facie* case of obviousness has not been made and the rejection of claim 8 under 35 U.S.C. § 103(a) should be withdrawn.

Discussion Regarding Patentability of Claims 9-14

Claims 9-14 depend from claim 8 and include the same limitation discussed above with respect to claim 8 and additional limitations. Therefore, for at least the same reasons set forth above with respect to claim 8, claims 9-14 are allowable over the prior art.

Discussion Regarding Patentability of Claim 10

Claim 10 depends from claim 8 by way of claim 9 and further recites generating a bogus request message. The Examiner has not identified any such limitation in the prior art. It is noted that the Examiner has alleged that "Cory et al. [teaches] transmitting

bogus messages in response to an actual message." (Office Action at page 4). However, even if accurate, there is no teaching or suggestion that the "actual message" is a "bogus request message" as claimed.

Moreover, the Examiner has clearly mischaracterized Cory. Specifically, the Examiner correctly notes that bogus data is transmitted during dead space between valid messages and subsequently the transmissions are received and decrypted at a receiver. (Office Action at page 4). However, the Examiner apparently proposes this as proof that the bogus messages were transmitted "in response to an actual message". In fact, as clearly recited by the Examiner and as discussed above, the bogus messages were transmitted *in response to the detected absence* of an actual message. Detecting the absence of a message does not teach or suggest that any actual message has been received.

Accordingly, in addition to the reasons set forth above, claim 10 is further allowable over the prior art.

Discussion Regarding Patentability of Claim 12

Claim 12 depends from claim 10 by way of claim 11 and further recites terminating the bogus message generation in response to a timer expiration. The Examiner has not identified any such limitation in the prior art. Accordingly, in addition to the foregoing reasons, claim 12 is further allowable over the prior art.

Discussion Regarding Patentability of Claim 13

Claim 13 depends from claim 10 by way of claim 11 and further recites terminating the bogus message generation in response to a bona fide transaction

occurring at a terminal where the bogus transactional message generation is occurring. The Examiner has not identified any such limitation in the prior art. Accordingly, in addition to the foregoing reasons, claim 13 is further allowable over the prior art.

D. Claims 16-20 Are Patentable Over the Proposed Combination

Discussion Regarding Patentability of Claim 16

Claim 16 recites a bogus message generator that generates bogus messages in accordance with parameters received in a "bogus request message". As set forth above with respect to claim10, the Examiner has not identified any such limitation in the prior art. Accordingly, claim 16 is allowable over the prior art.

Discussion Regarding Patentability of Claim 17

Claim 17 depends from claim 16 and includes the same limitation discussed above with respect to claim 16 and additional limitations. Therefore, for at least the same reasons set forth above with respect to claim 16, claim 17 is allowable over the prior art.

Discussion Regarding Patentability of Claim 18

Claim 18 recites terminating the bogus message generation in response to a timer expiration. The Examiner has not identified any such limitation in the prior art. Accordingly, in addition to the foregoing reasons, claim 18 is further allowable over the prior art.

Discussion Regarding Patentability of Claim 19

Claim 19 depends from claim 18 and includes the same limitation discussed above with respect to claim 18 and additional limitations. Therefore, for at least the same reasons set forth above with respect to claim 18, claim 19 is allowable over the prior art.

Discussion Regarding Patentability of Claim 20

Claim 20 recites terminating the bogus message generation in response to a bona fide transaction. The Examiner has not identified any such limitation in the prior art. Accordingly, in addition to the foregoing reasons, claim 20 is further allowable over the prior art.

V. Claims 21-25.

Claims 21-25 have been added. These claims recite novel and non-obvious limitations. Accordingly, claims 21-25 are believed to be allowable over the prior art.

VI. Conclusion

Applicant respectfully requests entry of the amendments and favorable consideration of the application.

A prompt and favorable action on the merits is requested.

Respectfully Submitted,
Maginot, Moore & Beck

March 11, 2005

James D. Wood
Attorney for Applicant
Attorney Registration No. 43,285

Maginot, Moore & Beck
Bank One Center Tower
111 Monument Circle, Suite 3000
Indianapolis, IN 46204-5115
Telephone: (317) 638-2922